Department of Public Health and Human Services (DPHHS)

Health Insurance Portability and Accountability Act ("HIPAA") Privacy Policy

John Chappuis, Deputy Director

Date: December 17, 2002

Revised Date:

Policy Title:	Employee Access to Protected Health Information (PHI)		
Policy Number:	013	**Version:**	1.0
Approved By:			
Date Approved:			

Purpose:

This policy addresses DPHHS employees' access to various levels of Protected Health Information ("PHI") as necessary to conduct their work.

Policy:

DPHHS employees will be granted access to the level of PHI that is necessary for them to accomplish their work.

Definitions for use in this policy (from the Information Security and Database Access Policy, 12-15-96).

1. Sensitivity Level 1: This is information of a general nature regarding the characteristics of the population served by a program. Data is presented in such a way that individual clients cannot be identified from analysis of the information. Examples include:

   a. AFDC population characteristics, such as the average length of stay, mean payment level and recidivism rate; and

   b. Medicaid client information such as the average age of clients, geographic distribution, and outcome analysis, such as the relationships between preventive services and cost of care.

   Basically, Level 1 information represents data summary type information rather than client specific data.

2. Sensitivity Level 2: This is the client demographic and basic service information. Generally, Level 2 demographic information is program specific and is limited to information necessary

to identify if an individual or family is known to the Department and to determine their program eligibility. Demographic information would be limited to:

a. Name, address, and phone number;
b. Date of birth; and
c. Social Security Number or other identification number.

Services information would be limited to the type of service(s) received or being received, dates of service(s) and the component within the Department providing the service(s). Level 2 information is considered "Confidential" in that the fact than an individual or family is known to the Department and has received or is receiving services is controlled by the Department on a need-to-know basis, but is not considered to be "sensitive" data in terms of the following Level 3 definition.

3. Sensitivity Level 3: Information at this level is detailed information about an individual client's personal background or previous and present services provided by the Department. Level 3 data are considered as "sensitive" data in that if the data are improperly used, serious damage could occur to the individual or family concerned. Examples of Level 3 information would include:

   a. Medical status and history including past and present conditions or illnesses;
   b. Specifics of medical diagnosis or tests;
   c. Treatment plans;
   d. Family background;
   e. Child support requirements and status, if appropriate;
   f. Financial status; and
   g. Specific information relative to the services provide by the Department.

4. DPHHS supervisors must determine which of their employees, if any, require access to PHI in order to do their work. Supervisors must then determine what level of PHI is REQUIRED by the employee to do that work.

5. The access sensitivity level should be written into the position description for future reference and for review by HIPAA enforcement agencies.

6. DPHHS employees will receive HIPAA training regarding PHI commensurate with their level of access. Supervisors will document the date of such training and communicate the training roster to the Privacy Officer. (See HIPAA policy #7 on Administrative Requirements 11-19-02 for frequency of that training.)

7. The employee level of access will be communicated to the Security Officer when computer access is requested.

8. Employees will be held accountable for their level of access, and uses and disclosures outside of that level will be considered grounds for potential sanctions. (See HIPAA policy #12 on Employee Sanctions 12-17-02.)

Procedure:

1. Each employee of MCDC will have a security sensitivity level assigned to him or her. The employee will have HIPAA training prior to April 14, 2003, during new employee orientation and yearly thereafter.
2. Employees will be tested after completing training. A copy of each employee's test with date of training, testing and employee's signature will be maintained in each employee's personnel record.
3. The original test will be routed to the State of Montana Privacy Officer.
    a. Yearly training and testing will follow procedures #2 and #3.
    b. Completed and signed test results will demonstrate that training has been fulfilled on a yearly basis.
4. A statement noting the security level of each position will be added to each employee's position description.